AUGUST 2024

Securing UAS Fleets from Cyber Attacks

Final Report

Benjamin Sugg, Steven Habicht, Riley Dove (RIIS, LLC),
and Andy Osantowske (NUAIR)

with contributions by Adam Monsalve, Addam Jordan, Marina Rozenblat,
Bayan Rustom, Jonathan Menna (RIIS, LLC), Godfrey Nolan (RIIS, LLC),
John Gustafson (NUAIR), Dan Waterman (NUAIR), Zevi Rubin (AX Enterprize),
and Brian Shoemaker (AX Enterprize)

IIM-2024-U-039129-Final

Abstract

As uncrewed aircraft systems (UAS) continue to proliferate in the National Airspace System (NAS) for both commercial and public safety operations, there has also been an increase in the number of potential cyber attacks that can be conducted on these systems. CNA, in collaboration with RIIS, LLC, NUAIR, AX Enterprize, and the New York UAS Test Site, conducted research and analysis focused on improving the safety of the NAS by identifying and mitigating vulnerabilities that can be addressed easily through UAS configuration changes. The Securing UAS Fleets from Cyber Attacks project is focused on addressing these issues by using the Brute Force Default Identification-Automated Prevention system to prevent brute force attacks through default setting identification on UAS platforms. This document provides an overview and final assessment of the activities leading to the final demonstrations at the UAS Test Site in Rome, New York, as well as an analysis of the data that were captured during the live operations.

This document contains the best opinion of CNA at the time of issue.

It does not necessarily represent the opinion of the sponsor or client.

Distribution: Approved for public release. Unlimited distribution.

This work was performed under Federal Aviation Administration Broad Agency Announcement Call 004,
Contract: 697DCK-23-C-00292.

Cover image: Jenn Karras, CNA.

Approved by: **August 2024**

Steven Habicht, Ph.D.
Director
Center for Enterprise Systems Modernization
CNA Institute for Public Research

Request additional copies of this document through inquiries@cna.org.

EXECUTIVE SUMMARY

As uncrewed aircraft systems (UAS) continue to proliferate in the National Airspace System (NAS) for commercial and public safety operations, the number of potential cyber vulnerabilities that malicious actors can exploit on these systems has also increased because of their networked communications. Many UAS vulnerabilities can be addressed easily through simple configuration changes, and UAS operators must harden their systems before flying. The "Securing UAS Fleets from Cyber Attacks" project addressed these issues by using the Brute Force Default Identification-Automated Prevention (BFDI-AP) system to prevent brute force attacks by identifying insecure default settings on selected UAS platforms that have been manufactured domestically or cleared by the Department of Defense's Defense Innovation Unit "Blue List." This automated solution is designed to secure UAS aircraft and fleets from cyber attacks and improve controls protection during UAS operations.

CNA, in collaboration with RIIS, LLC, NUAIR, AX Enterprize, and the New York UAS Test Site, conducted research and analysis focused on improving the safety of the NAS by identifying and mitigating vulnerabilities that can be addressed easily through UAS configuration changes. To secure these aircraft from cyber attacks, an automated solution was developed and validated through a series of live-flight demonstrations focused on public safety and commercial delivery scenarios. These demonstrations confirmed the BFDI-AP system in an operational environment. The BFDI-AP identified default configurations that are risks, mitigated the vulnerabilities through a configuration change, and communicated the change to the UAS operator. The scope of work included a vulnerability assessment, prototype system update, and test and evaluation through flight demonstrations. This project culminated in the successful live demonstration of the BFDI-AP system and the live flights of three commercial UAS platforms.

In addition to the enhanced and validated BFDI-AP security solution for UAS, our research resulted in recommendations to improve broader awareness among the UAS community of cybersecurity threats, vulnerabilities, and mitigations to improve the safety and security of these operations. This report details the approach, results, data, and challenges that resulted in the completion of the live demonstration at the UAS Test Site in Rome, New York, on July 16 and 17, 2024.

TABLE OF CONTENTS

This page intentionally left blank.

INTRODUCTION

The proliferation of uncrewed aircraft systems (UAS) within the National Airspace System (NAS) can be seen in a variety of applications ranging from agriculture to public safety, and in many cases, they have removed individuals from dangerous work, extended accessibility to remote locations, and increased the efficiency of various missions such as disaster relief and agricultural management. Although the benefits of commercial UAS are nearly innumerable, their widespread adoption has created a large attack surface subject to various cyber attacks. As with any other networked technology, UAS platforms are composed of hardware and software components that often contain misconfigurations and vulnerabilities. The successful exploitation of these systems can severely affect the confidentiality, integrity, and availability of system data and, in some cases, can lead to the loss of physical control of the UAS.

The "Securing UAS Fleets from Cyber Attacks" project sought to address these issues by using a countermeasure system to identify insecure default settings on commercial UAS platforms and update these settings automatically for the operator. This automated solution is designed to secure UAS fleets from cyber attacks and provide protection during UAS operations.

Background

In 2021, CNA partnered with software company RIIS (CNA-RIIS team) to complete the *NIST PSCR First Responder UAS Triple Challenge—Shields Up: Securing UAS Navigation and Control* [2]. Through a series of live UAS flights, the CNA-RIIS team demonstrated the real-world threat to UAS operations posed by a loss of command and control (C2) of their UAS. The team recognized the commonplace nature of simple security misconfigurations across various UAS platforms. To address this issue, the team developed the Brute Force Default Identification (BFDI) device, which takes advantage of poor cybersecurity practices and exploits known vulnerabilities from default settings found in common UAS technology. The team that developed the BFDI focused on compromising the control capabilities of the UAS, including the telemetry hardware on the UAS and the Wi-Fi or Bluetooth present within the ground control station (GCS). Using the device, the team forced a return to launch command, highlighting the public safety operator's loss of control, preventing the public safety operator from controlling the vehicle, and causing mission failure.

To counter cybersecurity attacks such as the one in that example, the CNA-RIIS team developed the BFDI–Automated Prevention (BFDI-AP) system. This preventive measure is applied to the UAS before launch. The system uses the same software as the attacking system, but rather than using it to compromise the UAS, the software automatically updates the misconfigured settings to secure the UAS against potential future attacks. The BFDI-AP system identifies default settings often vulnerable to brute force attacks on the platform and sends reconfiguration scripts that update the settings to a more secure state. Specifically, the system creates an automated feedback loop that checks for BFDI-related UAS vulnerabilities, makes corrections, and informs operators of any modifications via a user interface on the system to ensure that public safety organizations safely launch and complete their missions with a secure telemetry system.

The primary objective of the BFDI-AP system is to provide a user-friendly, efficient means for securing commercial small uncrewed aircraft system (sUAS) prior to conducting flight operations. As demonstrated in this report, many of these systems lack securely configured default settings out of the box, making the BFDI-AP system a tool that can rapidly addresses any "low-hanging fruit" that could be of interest to malicious actors.

Cybersecurity threats

UAS platforms are vulnerable to exploitation if not properly configured or patched. Attacks on these platforms include spoofing (mimicking or disguising identity), jamming (overwhelming the signal), code injection (inserting malicious code), remote access (accessing from a remote location), and data exfiltration (transporting data without authorization). For this project, the analysis focused primarily on the insecure misconfigurations that can be found in systems. They include the use of default credentials and nonrandomized identification mechanisms that malicious actors can exploit to gain control of the sUAS.

An analysis conducted by the Alliance for System Safety of UAS through Research Excellence considered threats to UAS throughout six operational phases: preflight/mission planning, preparation/system checks, launch, mission, application/flight/return to land, and postflight [3]. The authors concluded that UAS are at higher risk of cyber attacks after the system is launched and that "code and command injection, password cracking, and false data injection in sensor and database are high-risk factors for every phase of UAS's mode of operation." These findings clearly illustrate that UAS may be exploited in various ways and that such vulnerabilities must be identified and addressed quickly by remediation when possible. The use of the BFDI-AP system prior to operations mitigates the increased risks of sUAS being compromised while aloft.

Cybersecurity initiatives

The following sections introduce the Department of Defense's (DOD's) Defense Innovation Unit (DIU) Blue UAS List and the Association for Uncrewed Vehicle Systems International's (AUVSI) Green UAS List [4] initiatives; both are intended to verify federal and commercial UAS against cybersecurity requirements. Blue List UAS undergo cybersecurity assessments to protect sensitive military information and must meet DOD and National Defense Authorization Act (NDAA) requirements [5]. Although Green List UAS are not required to meet DOD requirements, the certification maintains high security for non-DOD customers. Both lists offer cybersecurity testing programs currently used in the UAS industry to validate the security and suitability of UAS for domestic UAS operations and ensure the prioritization of national security. These initiatives are mentioned because of their influence in scoping the project's analysis, and for this assessment, the testers excluded any UAS that would not meet the basic requirements of these standards (including foreign-made systems such as those manufactured by Da-Jiang Innovations (DJI)).

DIU Blue List

The Blue UAS List initiative is a program created by the DOD to identify and approve UAS for federal use. During vetting, UAS must meet strict security and operational standards to ensure that they are suitable for military applications and services. A Blue UAS List standing also implies compliance with the NDAA and ensures that the UAS has not been made, in parts or entirely, from a "covered foreign country," which could potentially create software vulnerabilities that compromise sensitive data and the networks they connect to, leading to potential national security threats. Blue UAS List standing and NDAA compliance ensure that organizations avoid acquiring UAS from countries that have interests counter to those of the US.

AUVSI Green List

The AUVSI Green UAS List is a component of AUVSI's Trusted Cyber Program and is integral to assessing and validating commercial drones. It supports DOD efforts to expand DIU's Blue UAS List with UAS that align with the same level of cybersecurity and supply chain management requirements mandated by Congress and the NDAA. This validation process involves security controls assessments, vulnerability testing, and penetration testing. The assessment process leverages the expertise of cybersecurity firms to rapidly vet UAS by addressing threats and risks in various domains, including corporate cyber hygiene, product and device security, and supply chain risk management. Obtaining Green UAS List status grants broader areas of sales to non-DOD clients who are permitted to purchase without an authority to operate but have an interest in strict cybersecurity vetting.

PROJECT OBJECTIVES

This project consisted of three primary objectives:

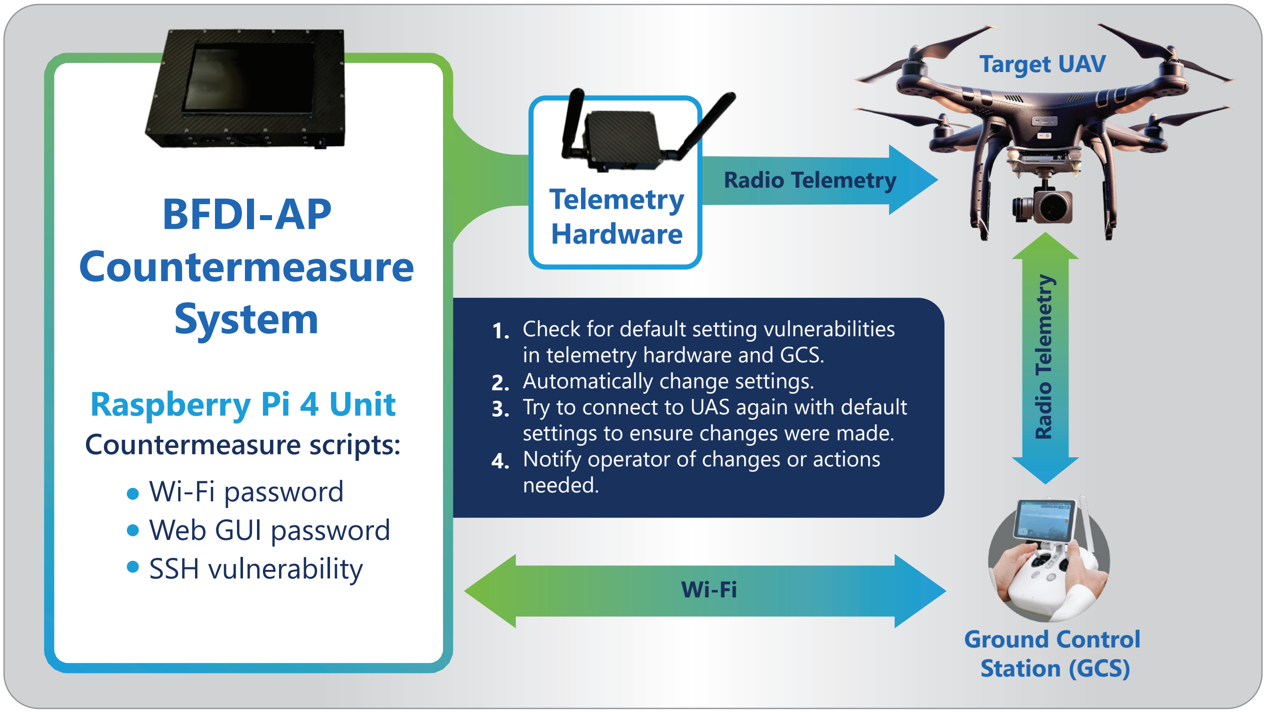
1. Provide a simple, automated solution to secure UAS aircraft and fleets from cyber attacks.
2. Improve the protection of C2 links during UAS operations.
3. Demonstrate and validate cyber technology to ensure uninterrupted UAS operations for commercial and public safety users.

Automated solution to secure UAS

The first objective consisted of developing and upgrading the BFDI-AP system. This system is an automated preventive countermeasure system to prevent brute force attacks through first identifying default setting and then executing automated scripts to randomize, and thus secure, the identified settings. The system's three core functions are to display vulnerabilities resulting from misconfigured UAS, mitigate identified vulnerabilities via configuration updates, and communicate the configuration updates to the UAS operator.

The system operational view for the BFDI-AP system is depicted in Figure 1.

Figure 1. BFDI-AP system operational view


BFDI-AP Countermeasure System
Raspberry Pi 4 Unit
Countermeasure scripts:
• Wi-Fi password
• Web GUI password
• SSH vulnerability
Telemetry Hardware
Radio Telemetry
Target UAV
Radio Telemetry
1. Check for default setting vulnerabilities in telemetry hardware and GCS.
2. Automatically change settings.
3. Try to connect to UAS again with default settings to ensure changes were made.
4. Notify operator of changes or actions needed.
Wi-Fi
Ground Control Station (GCS)

Source: CNA.

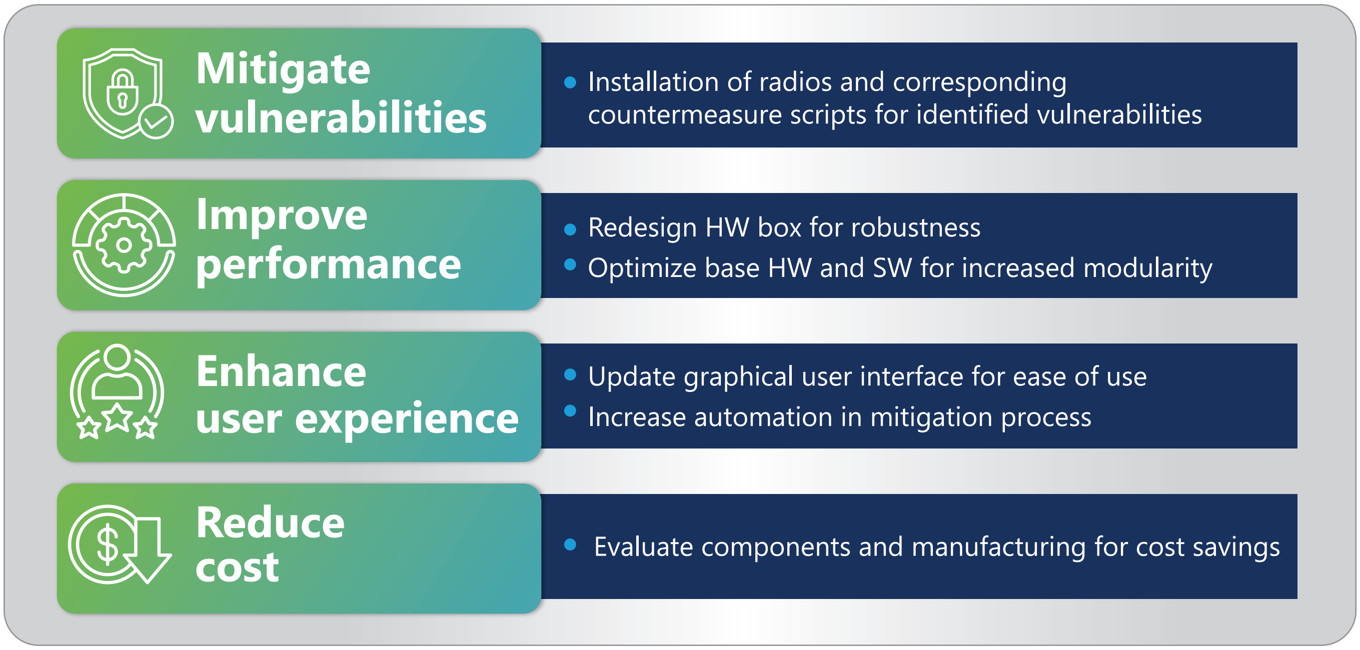
Protection of control links during UAS operations

For the second objective, a critical design review was conducted to improve the system and its ability to defend the protection of controls during UAS operations. This design review led to the prioritized enhancements shown in Figure 2.

Demonstration and validation of technology

The third objective was met by developing and executing real-world operational use cases for commercial and public safety scenarios. For the three UAS tested, each system underwent an initial "takeoff and land" flight, an "unprotected" flight with the default configurations, and a "protected" flight after the BFDI-AP scripts secured the system. All flight times and script execution times were recorded to validate the ease of use and efficacy of the technology.

Figure 2. BFDI-AP system enhancements from critical design review



Mitigate vulnerabilities

- Installation of radios and corresponding countermeasure scripts for identified vulnerabilities

Improve performance

- Redesign HW box for robustness
- Optimize base HW and SW for increased modularity

Enhance user experience

- Update graphical user interface for ease of use
- Increase automation in mitigation process

Reduce cost

- Evaluate components and manufacturing for cost savings

Source: CNA.

APPROACH

The UAS platforms analyzed during the multiple phases of this project were scoped to select systems that could be listed as policy-compliant under the DOD's Blue UAS List effort or the AUVSI Green UAS List. The radios used during the testing and demonstrations included the RFD900X and the Picoradio pMDDL 2450. These radios were key to validating that the BFDI-AP system communicated the updated security scripts properly to the sUAS systems. For security purposes, the manufacturers of the UAS that were analyzed during this project are anonymous in this report and will be notified of all security findings for remediation. The systems are identified by their corresponding radio components as well as whether their communications were Wi-Fi based.

These platforms and radios were procured from the manufacturers with the standard default settings to exemplify how many out-of-the-box systems contain default configurations vulnerable to exploitation. Furthermore, the scope of our testing was limited to identifying these misconfigurations and did not include software or firmware vulnerabilities because the BFDI system's capabilities are limited to the randomization of insecure settings and not applying software updates.

Project team

This project was a collaboration between CNA, RIIS LLC, NUAIR, AX Enterprize, and the New York UAS Test Site. CNA is a non-profit research and analysis organization with experience supporting government use of UAS and cybersecurity strategies. RIIS is a small business that specializes in mobile and artificial intelligence/machine learning applications for UAS. NUAIR is a non-profit organization that provides flight testing and validation for UAS and Advanced Air Mobility solutions. AX Enterprize is a small business technology firm that manages and coordinates the flight testing facilities at the New York UAS Test Site at Griffiss International Airport. The team members and capabilities that supported the efforts during the various stages of the project are listed in Table 1.

Vulnerability assessment

A vulnerability assessment was conducted on a select group of UAS compliant with either the DOD's DIU Blue UAS List effort or the AUVSI's Green UAS List effort. We subjected the five UAS systems to penetration testing techniques to identify exploitable vulnerabilities in the default settings.

Table 1. Project team and roles

Company	Program Management	Cybersecurity Research	Concept Development	Part 107 Operators	Hardware Development	Software Development	Flight Testing	Operations Center	UAS Test Site
CNA	✓	✓	✓	✓					
riis		✓		✓	✓	✓			
NUAIR			✓	✓			✓	✓	
AX Enterprize				✓			✓	✓	✓

Source: CNA.

Testing approach

Although the workflow of the tests conducted in this assessment was modified to meet the scope of the target systems, it is worth noting that most penetration tests are based generally on the Cyber Kill Chain Framework developed by Lockheed Martin [6]. Because of the limited scope and nature of the platforms that were tested in this assessment, the Cyber Kill Chain Framework methodology has been simplified into four steps: scanning and enumeration, exploitation, mitigation and remediation, and reporting (Figure 3).

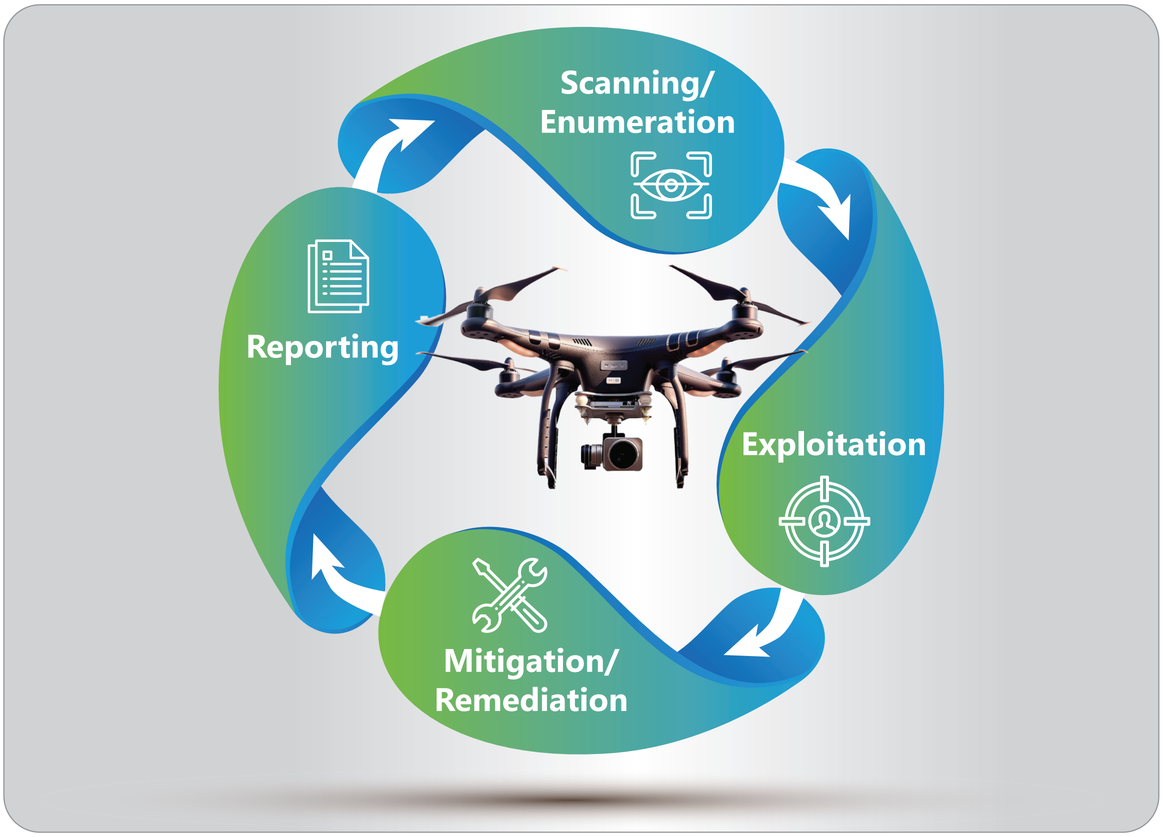
Scanning and enumeration

Much like the reconnaissance phase described in the Cyber Kill Chain Framework, the scanning and enumeration phase identifies potential vulnerabilities and weaknesses in the target system. This step can include passive information-gathering techniques that do not require direct engagement with the target (e.g., searching the internet for default credentials, system documentation) and active methods that involve contacting the target (e.g., Network Mapper scans, Burp Suite vulnerability scanner). This step aims to provide the tester with the greatest available amount of information to use in the exploitation phase.

Exploitation

After establishing a detailed understanding of the target system, which includes information such as open ports, running services, and application or program version information, the tester will evaluate where vulnerabilities might be available to exploit. Based on the data captured during the scanning and enumeration phase, this evaluation may be as simple as authenticating with default credentials because

Figure 3. Penetration testing methodology for UAS vulnerability assessment



Source: CNA.

of a misconfiguration or developing and using a software exploit on an identified vulnerability. If successful, this phase allows the tester to establish an initial foothold on the target system that can be used maliciously, including elevating privileges and exfiltrating data.

Mitigation and remediation

In the context of the scope of platforms tested in this assessment, this phase is unique because it involves using an automated preventive countermeasure system that mitigates identified vulnerabilities via configuration updates. The BFDI-AP system reconfigures those "low-hanging fruit" misconfigurations identified during the first phase and exploited during the second. It is important to note that the BFDI-AP system does not correct any potential software or firmware vulnerabilities that were identified during the scanning and enumerations phase and is not capable of issuing patches or updates; however, it does provide defense against brute force attacks through default setting identification, which is the primary attack vector in many of the use cases here.

Reporting

The final step in this process is the compilation of test findings, tools used, and techniques performed during the penetration test. The goal of this phase is twofold: to provide a transparent and detailed document that clearly illustrates how the vulnerabilities were found and exploited and to explain what was reconfigured successfully to a more secure state during the use of the BFDI-AP on the targets. In addition, remediation guidance on the vulnerabilities that were not fixed should be included for future system patching. The findings from this analysis will be compiled in an additional vulnerability database spreadsheet. As Figure 3 illustrates about penetration testing methodology, this process is typically iterative, but because of the scope of the current effort, the reporting phase is the final step for the platforms tested in this analysis.

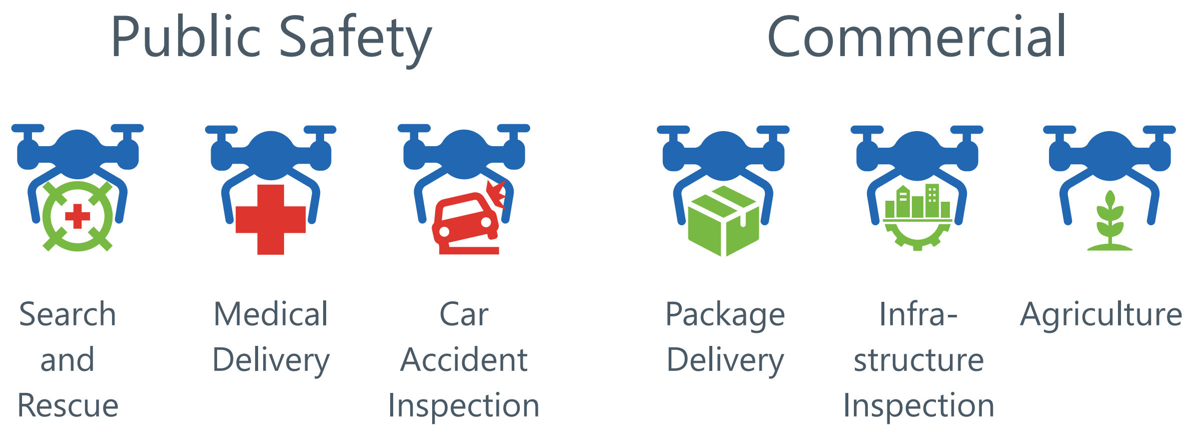
Testing tools

The scanning and enumeration phase of the penetration tests on the selected UAS required several well-known open-source tools. These tools are crucial to developing complete target system profiles. They are used to collect and organize information in an actionable way in the exploitation phase of the process. The three primary tools used in this assessment were Zenmap, Legion, and the Burp Suite vulnerability scanner, which we chose because of their open-source and highly documented nature, ease of use, and ability to capture network data from accurately the tested platforms.

Use case development

UAS have revolutionized many industries with their versatility and adaptability. UAS showcase their potential and reliability in various sectors and applications ranging from surveillance and reconnaissance to agriculture, construction, and emergency response. As technological advancements continue to propel the capabilities of UAS, their use cases continue to expand, reshaping the way industries approach challenges and use transformative technologies for emerging missions. The use cases selected for this project illustrate how UAS systems can increase the efficiency and efficacy of public safety and commercial operations. Compromising UAS by exploiting vulnerabilities and misconfigurations could severely degrade or terminate UAS missions crucial for protecting the public and increasing efficiency in commercial business. We selected a breadth of UAS use cases across public safety and commercial operations to demonstrate the application of the BFDI-AP system to protect these operations. The use cases that were selected for the demonstration scenarios are shown in Figure 4.

Figure 4. UAS use cases for BFDI-AP demonstration



Source: CNA.

Public safety: search and rescue

Using rapid-deployable platforms, search and rescue operations can occur anywhere and at any time. This scenario will focus on the quick-response capabilities of a small UAS to deploy and begin capturing potentially lifesaving data for dissemination among responding units. Although similar to other public safety scenarios, the flight profile of this use case will be more reactive and sporadic, similar to real-world operations.

Public safety: medical delivery

Many first-response use cases using UAS strive to combine critical first-on-scene equipment delivery with the ability to locate and transmit the location of the subject(s) and provide a real-time feed of the scene, the subject(s), and the surrounding environment. Armed with this real-time data, first responders can better decide the appropriate response type and size, especially if operating in forward or desolate response locations. They can also be better prepared to take protective measures required by the environment, such as large gatherings of people, nearby wildlife, or other hazards. This scenario simulated UAS providing lifesaving supplies critical to the survival of first responders on the ground via a traditional delivery profile. The UAS will hover at altitude to simulate lowering a package and immediately climb and orbit to simulate the transition to an overwatch operation.

Public safety: car accident inspection

During accident or incident response and reconstruction, first-response agencies often work collaboratively to secure the scene of an accident by first attending to first aid priorities, followed by seeking to understand what caused this event and what occurred because of it. By using UAS technology, first responders can expend dramatically less time, resources, and space to safely capture the images needed to better understand what occurred or the conditions that contributed to the accident. This demonstrated use case will simulate the flight profiles likely to be flown during accident response and reconstruction, including point-to-point flight maneuvers with loitering of varying altitudes for image or video capture.

Commercial: package delivery

Package delivery is one of the widely publicized use cases for commercial UAS. Many leading retail and shipping companies are entering this market to varying degrees. Common elements among most (if not all) of these current operations include short- to mid-mile delivery distances, payload weight limitations, and flights within more populated geographies. In this scenario, the UAS will largely follow a common flight profile. The vehicle will enter the delivery location at a safe transversing speed and en route altitude for this operation, descend vertically to the delivery altitude, lower the package (simulated) while hovering in place, ascend vertically back to a safe en route altitude, and depart the area.

Commercial: structure inspection

Early in the development of this technology, UAS demonstrated their usefulness for real estate because they can take images and video that would otherwise be too expensive or difficult to capture. This scenario simulates flights around a fixed structure at various angles, altitudes, and speeds to mimic common flight profiles when UAS gather images and video.

Commercial: agricultural management

Another commercial use of UAS to consider is agricultural management, including data collection on soil conditions, irrigation, and plant health. Through high-resolution imagery and data, UAS can monitor crop health and water quality in real time.

They can also optimize production while minimizing resource wastage through precision agriculture with the data captured.

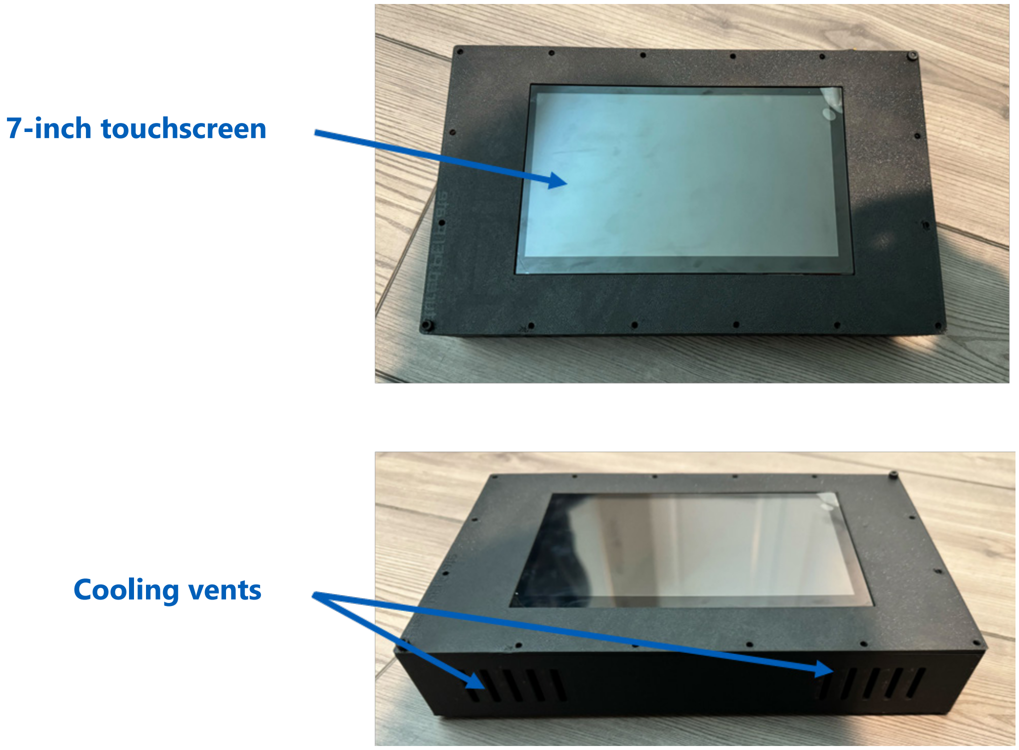
Data collection and analysis plan

A data analysis plan was developed to outline the project's approach to data collection. This document identified the data we gathered via Wi-Fi and radio frequency enumeration methods during the various phases of the penetration tests we conducted on the UAS. The data we collected from these tests clearly illustrated the pervasiveness of poor security controls and misconfigurations among commercial UAS platforms when basic security configurations are not addressed.

System design

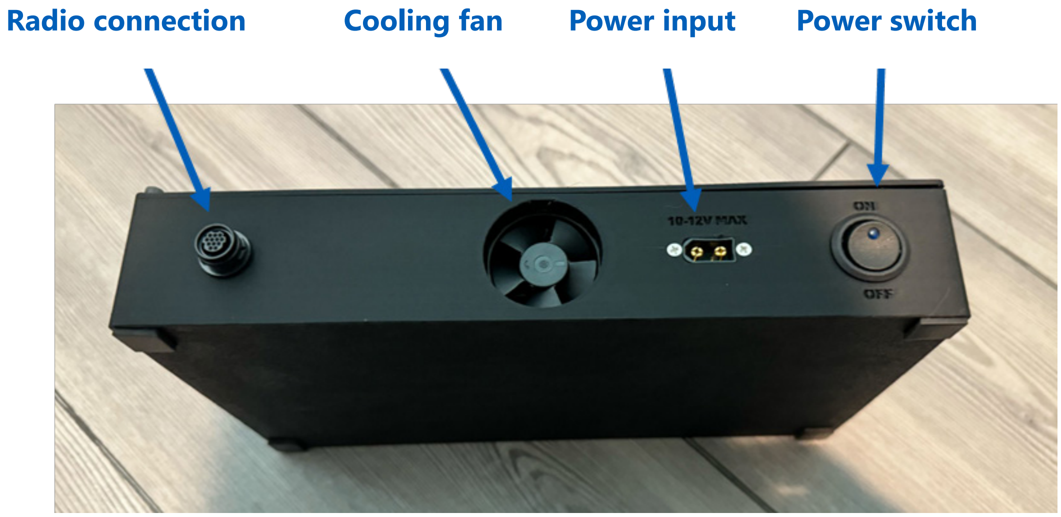
A critical design review evaluated the current BFDI-AP prototype against two criteria: the vulnerabilities found in the vulnerability assessment and the performance requirements listed in the data analysis plan. In addition, this document determined the key design considerations to meet the project objectives and prepared the updated BFDI-AP system design. The system updates that resulted from the review included the addition of a Wi-Fi dongle to enable Wi-Fi connection to UAS platforms, more cooling vents for additional airflow, code for Wi-Fi connectivity, and both tested radios' default settings to the system, as well as improvements to the user interface. The updated BFDI-AP system and its components are shown in Figure 5, Figure 6, Figure 7, and Figure 8.

Figure 5. BFDI-AP system (front view)



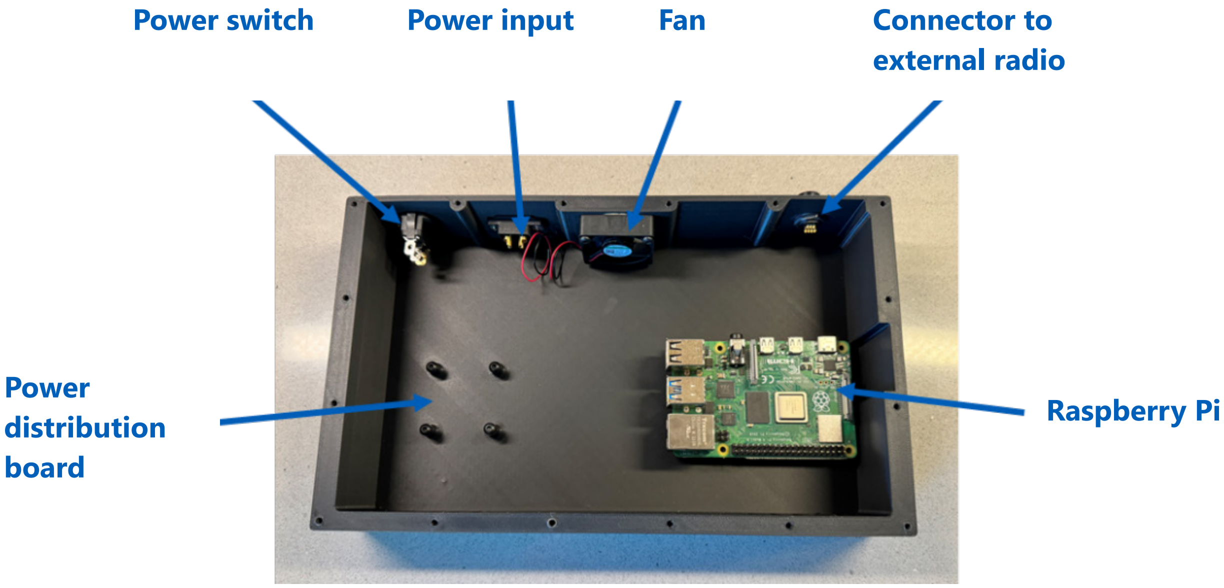
Source: CNA.

Figure 6. BFDI-AP system (top view)



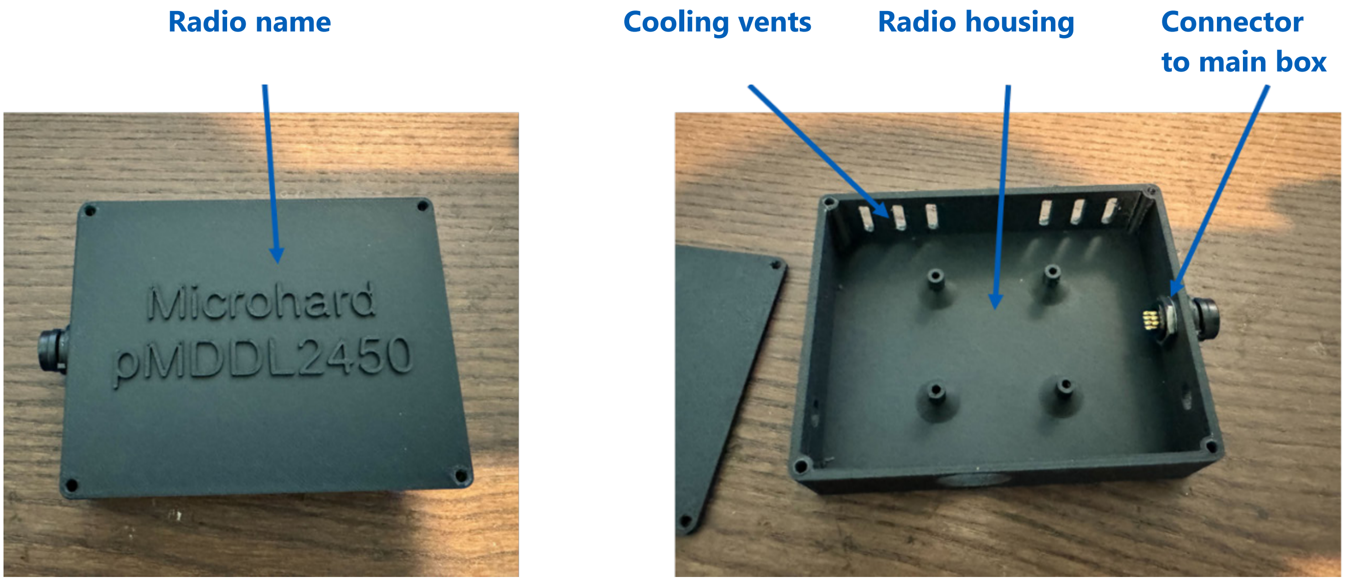
Source: CNA.

Figure 7. BFDI-AP system (internal view)



Source: CNA.

Figure 8. BFDI-AP system (radio box)



Source: CNA.

Test and evaluation

We developed a flight test plan to describe the approach and procedures that the project team will use to demonstrate the capabilities and performance of the updated BFDI-AP system. We described the scenarios for the live-flight demonstrations that would be used to highlight the vulnerabilities and efficacy of the BFDI-AP prototype. The approach included commercial and public safety scenarios in our live-flight demonstrations and featured UAS appropriate for each use case. The scenarios were designed to demonstrate how the systems operate in vulnerable, compromised, or remediated states and to avoid any in-flight attacks to ensure the safety of the operators and ground crew.

Demonstration planning

Following completion of the vulnerability assessment and the data analysis plan, the project team met near Syracuse, New York, in early 2024 to review the flight test plan for the project and the final demonstration scheduled for July 2024. The discussion covered project requirements and outcomes (especially those related to the base flight testing and the final demonstration), the design and development status of the system, Federal Aviation Administration (FAA) test site coordination and information sharing, and safety and airworthiness requirements.

Before this event, we discovered a potential safety hazard when using the BFDI-AP system on a sUAS that was aloft. At one point, when the

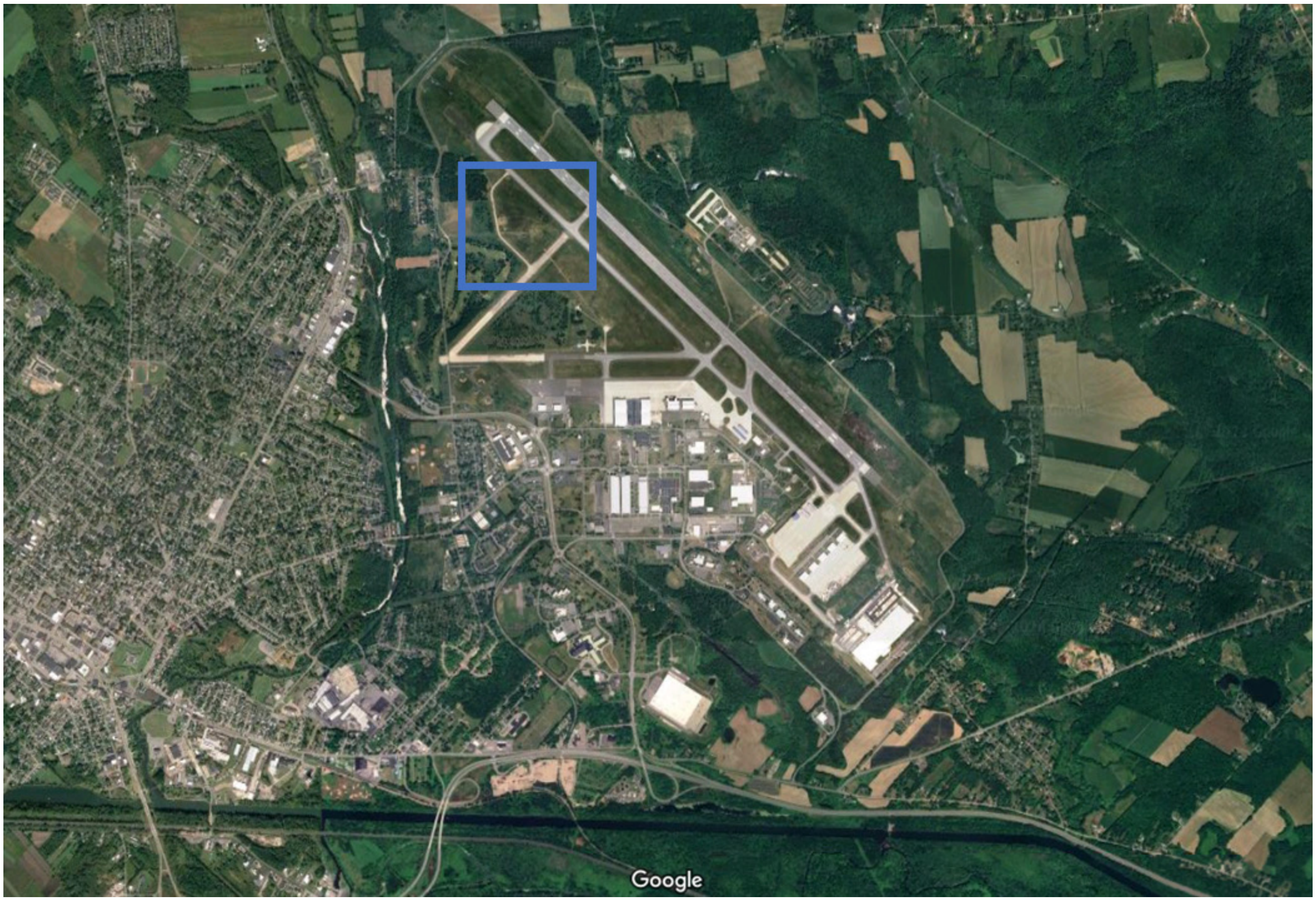
BFDI-AP protocols had been successfully applied, the controller inputs were unintentionally reversed resulting in an unsafe flying environment for both participants and nonparticipants. We discussed this finding at length with multiple flight safety and vehicle airworthiness experts who were well-versed in testing compromised UAS platforms and associated technologies when flying them, which is neither advised nor recommended. To ensure safety during the final demonstration, we did not conduct any in-air compromise of UAS flights.

During this planning event, we also focused on generating the flight requirements and creating an initial timeline of activities for the final demonstration. We recognized that accomplishing 40 total flights of 15 minutes each would create multiple technical and schedule risks, requiring adjustments to mitigate safety hazards and meet contract requirements. Examples of technical risks include managing the batteries, including charging and recharging cycle times with limited flight duration, and ensuring that the vehicle is airworthy and safe following configuration changes. These technical risks then create schedule risks in the timeline of events. We had to consider how best to demonstrate and explain the BFDI-AP process to those attending within a reasonable amount of time while planning for weather contingencies and other unforeseen delays. To mitigate these risks, we will conduct and film most of the test and demonstration flights before the final demonstration event to ensure that we meet project requirements and mitigate any technical, schedule, or other contingencies that may arise.

DEMONSTRATION AND VERIFICATION

On July 16 and 17, 2024, CNA and RIIS, LLC conducted a live demonstration of the BFDI-AP system on the selected UAS platforms at the FAA-designated New York UAS Test Site located at the Griffiss International Airport in Rome, New York (see Figure 9). The New York UAS Test Site, owned by Oneida County, provided the pilots and demonstrators with ample outdoor space for the event and the infrastructure necessary for public safety and commercial scenarios. All flights and BFDI-AP scripts were logged during the demonstrations, and a live videography crew filmed all the scenarios.

Figure 9. Satellite view showing the New York UAS Test Site at Griffiss International Airport in Rome, New York



Source: Google Maps.

Note: The blue box indicates the primary area used for testing.

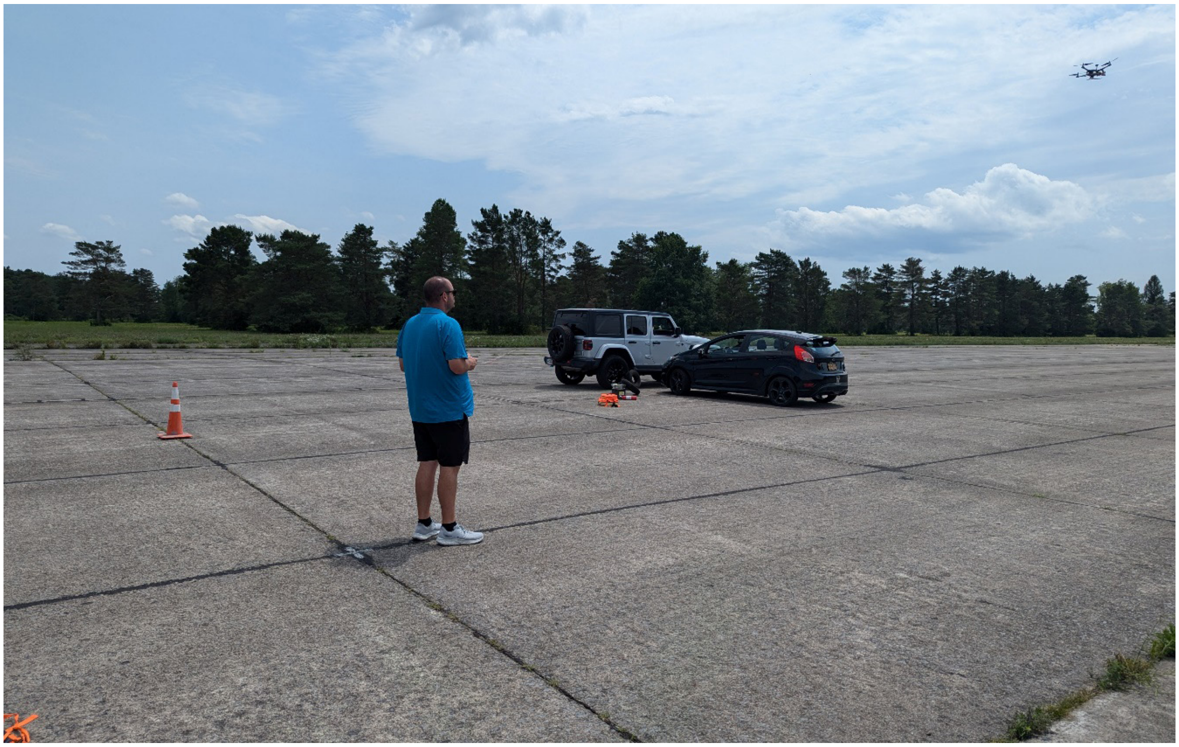
Demonstration Day 1

Day 1 of the demonstrations consisted of the following schedule:

- Test site arrival and security screening (security processing and visitor credentialling were required for all attendees)
- Welcome and introductions
- Project overview
- "Dry run" flights that included protected and unprotected flights of all three UAS platforms

Following the mandatory security screening and introductions, members of CNA and RIIS prepared the selected UAS. They conducted a series of dry run and short takeoff and land flights for each platform to ensure that all equipment worked safely and properly. The takeoff and land flights were short, approximately 30-second flights in which each system was powered on, paired to the corresponding GCS, armed, flown vertically to a maximum of 10 feet, and landed. These takeoff and land flights did not use the BFDI-AP system and were deemed unprotected. The dry run demonstrations consisted of four flights for each platform: one commercial scenario unprotected, one commercial scenario protected, one public safety scenario unprotected, and one public safety scenario protected. The protected flights took place after the BFDI-AP security scripts successfully randomized the default settings on each platform. Figure 10 shows an example of one of the dry run UAS flights the team performed during Demonstration Day 1.

Figure 10. Dry run UAS flight demonstrating the car accident inspection scenario performed during Demonstration Day 1



Source: CNA.

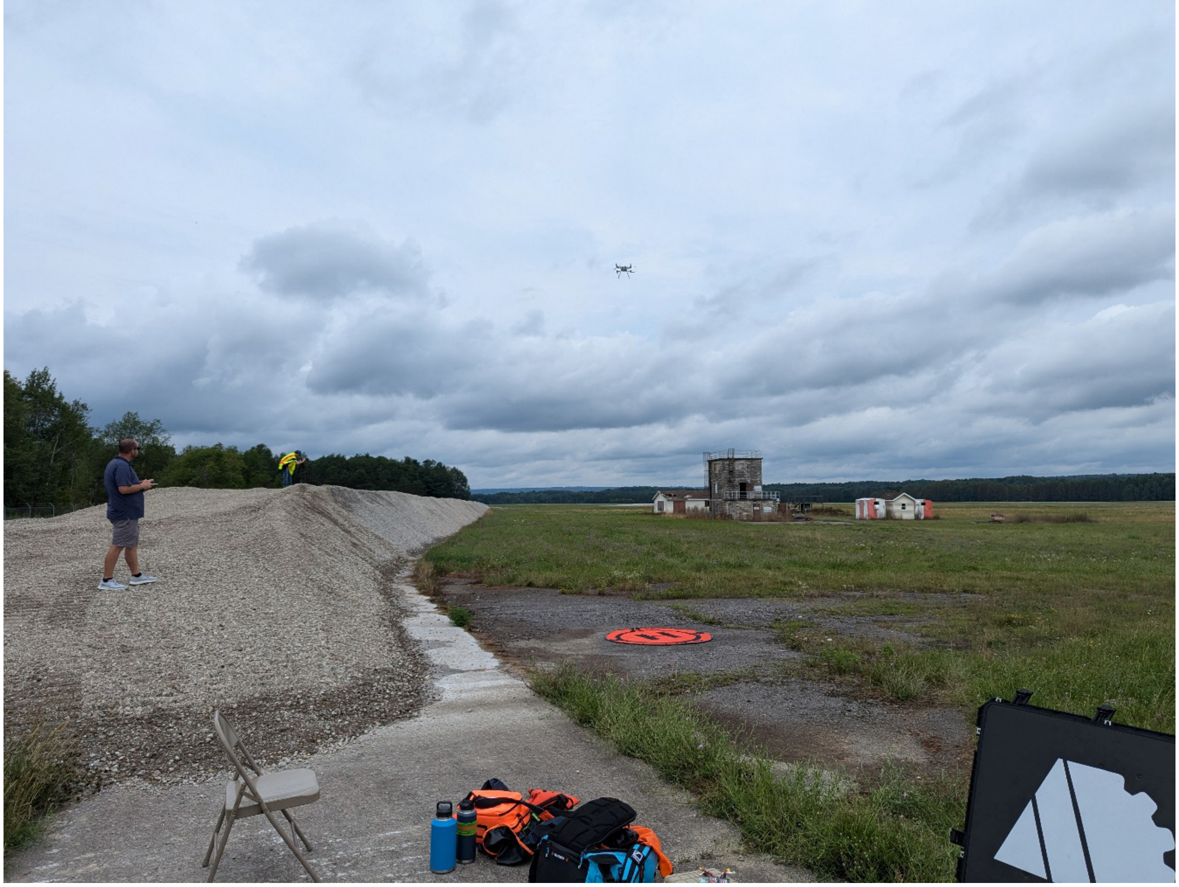
Demonstration Day 2

On the second day of demonstrations, all platforms were subjected to the same criteria as the dry run flights the day before, and additional infrastructure provided by the test site was used to enhance each scenario. All flights and scripts were logged and recorded by the videography crew. The following scenarios were completed successfully:

- UAS: pMDDL2450—Public Safety: Search and Rescue
- UAS: RFD900—Commercial: Package Delivery
- UAS: RFD900—Public Safety: Medical Delivery
- UAS: Wi-Fi (1)—Commercial: Infrastructure Inspection
- UAS: Wi-Fi (1)— Public Safety: Car Accident Inspection

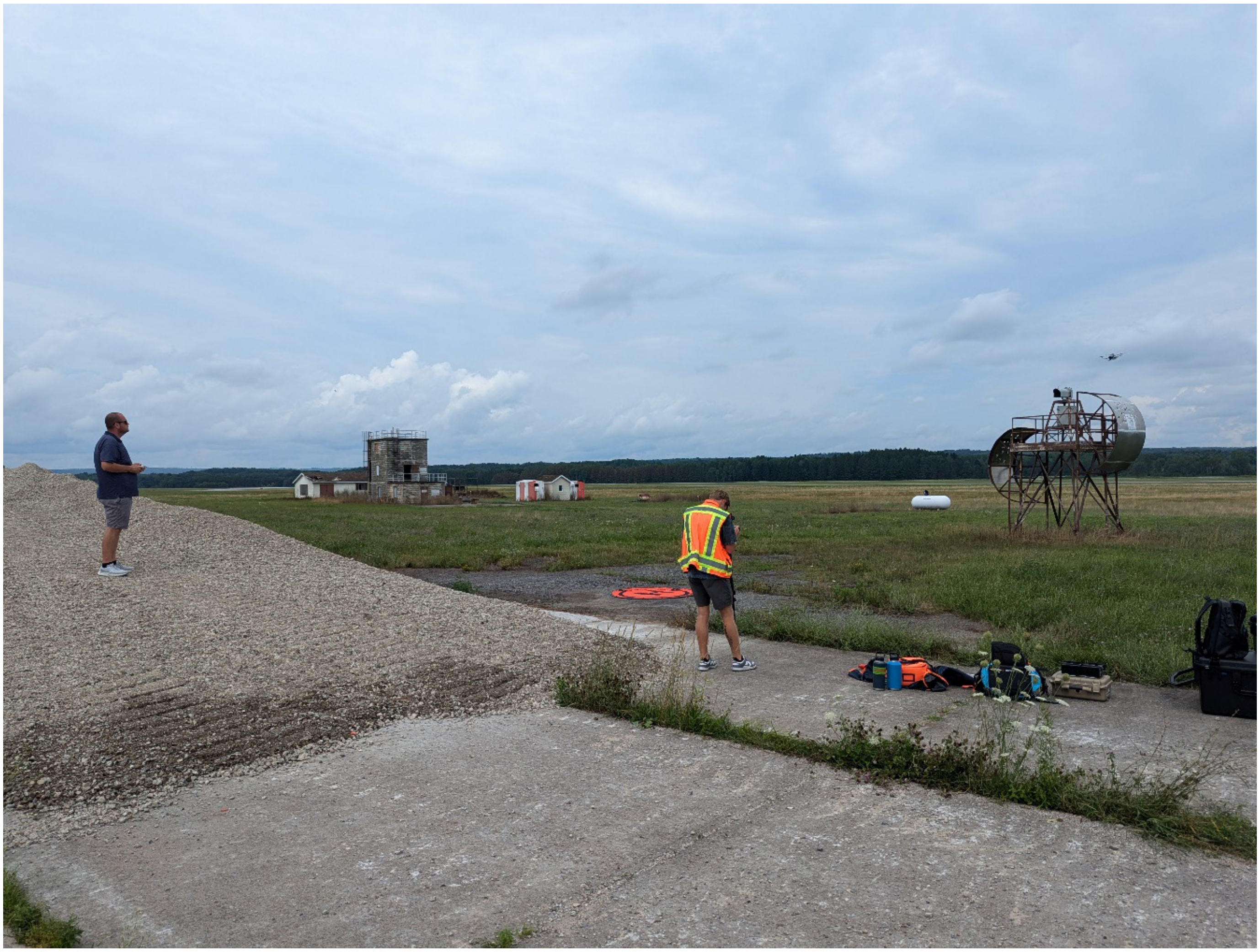
Figure 11 and Figure 12 show examples of the UAS flights the team performed during Demonstration Day 2 to demonstrate these scenarios.

Figure 11. UAS flight demonstrating the package delivery scenario performed during Demonstration Day 2



Source: CNA.

Figure 12. UAS flight demonstrating the infrastructure inspection scenario performed during Demonstration Day 2



Source: CNA.

DATA ANALYSIS AND RESULTS

Our project began with a vulnerability analysis to identify security misconfigurations in commercially available UAS platforms. This analysis set the scope of platforms to be used in subsequent flight testing and demonstration activities. During the initial testing conducted in Troy, Michigan, and the final demonstrations in Rome, New York, the CNA and RIIS teams logged all flights and BFDI-AP scripts. The following subsections present an overview of the activities conducted at each stage, the data collected from these activities, and the key findings from analyzing the data.

Vulnerability analysis findings

Our vulnerability analysis was a key first step in identifying the security vulnerabilities and misconfigurations from the penetration tests on each system. Although various security issues were identified during the testing phase, the three primary misconfigurations were within the default SSID, default login credentials, and default root credentials. Table 2 shows the prominence of these misconfigurations across each analyzed UAS.

Based on our findings from this analysis, the three platforms chosen to demonstrate the updated BFDI-AP system capabilities were the UAS: Wi-Fi (1), UAS: pMDDL2450, and UAS: RFD900. The UAS: Wi-Fi (3) was excluded from the analysis because of its overall robust security, including that the default password was both randomized and included in the packaging of the device, which would have required that a malicious actor obtain physical access to the system prior to any flights. UAS: Wi-Fi (2) was excluded based on the redundancy of its features that were also found in the more commonly used UAS: Wi-Fi (1). After testing both of these systems, it became clear that, for demonstration purposes, selecting the more commonly used drone made more sense than simply repeating the BFDI-AP script on a nearly identical system.

Table 2. Primary security misconfigurations found in UAS platforms (denoted by ●)

Platform	Default SSID	Default Login Credentials	Default Root Credentials
UAS: Wi-Fi (1)	●	●	●
UAS: Wi-Fi (2)	●	●	●
UAS: pMDDL2450	—	●	●
UAS: Wi-Fi (3)	●	—	—
UAS: RFD900	—[a]	—	—

Source: CNA.

[a] Although not a default SSID, the UAS: RFD900 broadcasted its NetID that could be matched with the correct channel and frequency to grant access to an unauthorized user.

Testing activities: RIIS in Troy, Michigan

In late May and June, members of the CNA, RIIS, and NUAIR teams met in Troy, Michigan, at the RIIS offices to conduct initial testing on the BFDI-AP system and the platforms that were eventually used during the demonstrations in Rome, New York. During these trips, the UAS: RFD900 , UAS: pMDDL2450 , and UAS: Wi-Fi (1) were all subjected to numerous flights that familiarized the pilot with basic maneuvers and simulated test flights in preparation for the final scenarios. Each system was flown unprotected (pre-BFDI-AP) and protected (post-BFDI-AP).

Table 3 summarizes the flight data collected from the test flight log. The success and failure columns indicate whether the drone had completed the test flight.

As shown in Table 3, the majority of the 38 flights conducted during this testing period were successful. These flights' brief average flight times resulted primarily from time constraints from inclement weather in the testing area and the purpose of quickly demonstrating and confirming the functionality and reliability of all the selected systems. The failed flight for UAS: pMDDL2450 occurred because of the BFDI-AP system's failure to initially connect to the local radio. UAS: RFD900 failure was caused by human error in failing to capture the randomized encryption key and network ID following the execution of the BFDI security scripts. Table 4 summarizes the BFDI-AP security scripts run during the testing in Troy, Michigan.

As Table 4 illustrates, the BFDI-AP system was largely successful in correctly executing the security scripts to randomize the default settings on the tested platforms. The three failures during this testing led to several troubleshooting rounds and the eventual identification and remediation of issues within the scripts.

Dry runs at New York UAS Test Site

Before conducting the final demonstrations, the CNA and RIIS teams conducted dry run flights and BFDI-AP script executions. The teams ensured that the systems were functioning correctly on site and that the scenarios could be executed successfully for each platform. Each UAS went through a series of flights, including protected and unprotected commercial and public safety scenarios and initial brief takeoff and land tests.

Table 3. Flight data from testing at RIIS Facilities, May and June 2024

Platform	Total	Average Time	Success	Fail	Unprotected	Protected
UAS: pMDDL2450	15	1:22	14	1	11	4
UAS: RFD900	17	1:25	16	1	12	4
UAS: Wi-Fi (1)	8	0:14	8	0	1	7

Source: CNA.

Table 4. BFDI-AP security script data from testing at RIIS facilities, May and June 2024

Platform	Total	Average Time	Success	Fail
UAS: pMDDL2450	5	2:15	4	1
UAS: RFD900	12	2:15	10	2
UAS: Wi-Fi (1)	6	0:38	6	0

Source: CNA.

Table 5. UAS: pMDDL2450 flight data from dry runs in Rome, New York

Flight Time	Type and Scenario	Success	Fail	Unprotected	Protected
00:38	**Takeoff & Land** Scenario: NA	✓		●	
2:10	**Commercial** Scenario: Agriculture	✓		●	
NA	**Commercial** Scenario: Agriculture		✗		●
NA	**Public Safety** Scenario: Search and Rescue		✗	●	
NA	**Public Safety** Scenario: Search and Rescue		✗		●

Source: CNA.

UAS: pMDDL2450 dry run results

Table 5 contains the flight results for the UAS: pMDDL2450 during the testing/dry run day at the test site.

As shown in Table 5, the UAS: pMDDL2450 was flown successfully for the initial takeoff and land flight. Following the initial functionality test, the drone successfully flew an unprotected agricultural inspection flight above a field for just over two minutes. After completing the unprotected commercial flight, the UAS failed to pair with the controller. This issue led the team to spend time troubleshooting the issue, and, as a result of weather conditions and time constraints, the additional dry run flights were not completed.

Table 6. UAS: RFD900 flight data from dry runs in Rome, New York

Flight Time	Type and Scenario	Success	Fail	Unprotected	Protected
00:36	**Takeoff & Land** Scenario: NA	✓		●	
1:47	**Commercial** Scenario: Package Delivery	✓		●	
2:02	**Commercial** Scenario: Package Delivery	✓			●
2:10	**Public Safety** Scenario: Medical Delivery	✓		●	
1:53	**Public Safety** Scenario: Medical Delivery	✓			●

Source: CNA.

UAS: RFD900 dry run results

Table 6 contains the flight results for the UAS: RFD900 during the testing/dry run day at the test site.

The dry run flights for the UAS: RFD900 were all successfully executed. Following the initial takeoff and land flight, the pilot conducted a short, unprotected commercial flight that simulated the delivery of a package with the UAS. Upon landing, the BFDI-AP system was used to randomize the default settings on the system. We then conducted a protected flight to demonstrate that the system maintained its operational integrity after running the security script. Following the commercial dry runs, the same process was successfully conducted for the public safety scenario, which simulated the delivery of medical supplies. As with the commercial flights, the unprotected and protected operations were successful, as was the execution of the security script.

UAS: Wi-Fi (1) dry run results

Table 7 contains the flight results for the UAS: Wi-Fi (1) during the testing/dry run day at the test site.

The initial UAS: Wi-Fi (1) takeoff flight was successful and confirmed the functionality of the UAS. The first dry run flight for the system was a commercial-based scenario in which the drone simulated the inspection of a structure. The unprotected and protected commercial flights were successful, as was the execution of the BFDI-AP security script. The public safety dry run flights were also successful, and for this scenario, two vehicles were staged to simulate a car accident. Because of unforeseen time constraints during the following day, these flights were considered sufficient for the live demonstrations and were not repeated.

Table 7. UAS: Wi-Fi (1) flight data from dry runs in Rome, New York

Flight Time	Type and Scenario	Success	Fail	Unprotected	Protected
0:23	**Takeoff & Land** Scenario: NA	✓		●	
00:55	**Commercial** Scenario: Structure Inspection	✓		●	
00:51	**Commercial** Scenario: Structure Inspection	✓			●
1:50	**Public Safety** Scenario: Car Crash Inspection	✓		●	
1:14	**Public Safety** Scenario: Car Crash Inspection	✓			●

Source: CNA.

Script data from the dry run day

As shown in Table 8, the CNA and RIIS teams had difficulty successfully executing the BFDI-AP security script on the UAS: pMDDL2450 system. A total of six attempts were conducted, with only one success. The team spent time troubleshooting this issue, and it was ultimately determined that the incorrect encryption key was entered on the BFDI-AP user interface, which did not allow the system to correctly pair following the randomization of the default settings. The BFDI-AP scripts for the UAS: RFD900 and the UAS: Wi-Fi (1) were all successfully executed, and as shown in the data, the UAS: Wi-Fi (1) had by far the fastest script runtime.

Table 8. BFDI-AP script data from dry runs in Rome, New York

Platform	Total	Average Time	Success	Fail
UAS: pMDDL2450	6	1:02	1	5
UAS: RFD900	3	1:38	3	0
UAS: Wi-Fi (1)	3	00:39	3	0

Source: CNA.

Table 9. UAS: pMDDL2450 final demo flight data

Flight Time	Type and Scenario	Success	Fail	Unprotected	Protected
NA	**Commercial** Scenario: Agriculture		✗	●	
NA	**Commercial** Scenario: Agriculture		✗		●
2:38	**Commercial** Scenario: Search and Rescue	✓		●	
4:11	**Public Safety** Scenario: Search and Rescue	✓			●

Source: CNA.

Final demonstrations at the New York UAS Test Site

UAS: pMDDL2450 final demo results

Table 9 contains the flight results for the UAS: pMDDL2450 during the final demonstration day at the test site.

The UAS: pMDDL2450 flight results for the final demonstration were 50 percent successful. The first flights of the morning were the unprotected and protected public safety search and rescue operations. For this scenario, the UAS was flown a considerable distance from the operator in a rural setting to simulate the drone's capability of locating a missing individual. Both flights were successful, and the BFDI-AP script was executed without issues. After landing the drone following the protected public safety flight, the system could not pair back to the GCS. After spending time troubleshooting the issue, the team decided to move on to the other platforms; therefore, the commercial scenario flights were not conducted successfully.

UAS: RFD900 final demo results

Table 10 contains the flight results for the UAS: RFD900 UAS during the final demonstration day at the test site.

The UAS: RFD900 UAS was flown successfully for protected and unprotected commercial and public safety scenarios. The commercial scenario was a package delivery operation in which the UAS was flown between two locations, descended to a drop-off location, and then flown back to the takeoff area. The medical delivery scenario was demonstrated similarly. The BFDI-AP security scripts were successfully executed for both scenarios, and the script logs were saved.

UAS: Wi-Fi (1) final demo results

Table 11 contains the flight results for the UAS: Wi-Fi (1) during the final demonstration day at the test site.

As noted in the dry run section, the final demonstration flights conducted by the UAS: Wi-Fi (1) consisted of the commercial structure inspection scenario. The previous day's flights for the car crash inspection were

Table 10. UAS: RFD900 final demo flight data

Flight Time	Type and Scenario	Success	Fail	Unprotected	Protected
2:24	**Commercial** Scenario: Package Delivery	✓		●	
4:35	**Commercial** Scenario: Package Delivery	✓			●
2:59	**Public Safety** Scenario: Medical Delivery	✓		●	
2:29	**Public Safety** Scenario: Medical Delivery	✓			●

Source: CNA.

Table 11. UAS: Wi-Fi (1) final demo flight data

Flight Time	Type and Scenario	Success	Fail	Unprotected	Protected
1:46	**Commercial** Scenario: Structure Inspection	✓		●	
1:17	**Commercial** Scenario: Structure Inspection	✓			●
1:50	**Public Safety** Scenario: Car Crash Inspection	✓		●	
1:14	**Public Safety** Scenario: Car Crash Inspection	✓			●

Source: CNA.

deemed to be sufficient for the public safety scenario. For the structure inspection, the drone was flown near a dilapidated building on the test site to examine the structure for construction defects. The unprotected and protected flights were conducted successfully, and the BFDI-AP security scripts ran correctly.

Script data from final demonstration

As shown in Table 12, the BFDI-AP security script was successfully executed in five out of six attempts during the final demonstration. The one failure was on the UAS: pMDDL2450 platform following the successful search and rescue scenario flights. The scripts for the UAS: RFD900 and the UAS: Wi-Fi (1) were executed successfully. Similar to the tests conducted during the dry runs, the UAS: Wi-Fi (1) was the fastest in randomizing its default settings.

Demonstration summary

Throughout the two-day dry runs and final demonstrations at the UAS Test Site in Rome, New York, the CNA and RIIS teams conducted 20 successful flights and 13 successful BFDI-AP security script demonstrations. Although most of the operations were performed without issue, the data presented here show that multiple technical difficulties inhibited the full demonstration of the UAS: pMDDL2450 drone. After completing the final scenario flights for the other UAS, the UAS: pMDDL2450 was analyzed to identify and remediate the issues experienced throughout the demonstration. This troubleshooting process revealed that some of the configurations on the radio did not match those on the UAS (frequency, channel, and encryption algorithm), which are necessary for pairing the devices successfully, and that a serial command was necessary to complete the syncing process.

Table 12. BFDI-AP script data from final demo in Rome, New York

Platform	Total	Average Time	Success	Fail
UAS: pMDDL2450	2	1:34	1	1
UAS: RFD900	2	1:42	2	0
UAS: Wi-Fi (1)	2	00:40	2	0

Source: CNA.

CHALLENGES

During the project, we encountered several challenges that had the potential to affect our objectives and results:

- Signal interference
- UAS flyability
- UAS configurations
- Safety concerns
- Supply chain delays
- Weather effects
- Distributed project team

One of the key challenges our project team encountered was the impact of **signal interference** from WIFI and RF signals with our BFDI-AP system countermeasure scripts. When performing our initial tests of the BFDI-AP scripts on the UAS platforms, we found that several of the tests would intermittently fail. Through our troubleshooting process, we found that when we performed the test outdoors (i.e., outside of the lab setting), the scripts worked more reliably. This will be a key area for future research to inform the scalability of this system to UAS fleets.

Another challenge our team realized during the testing process was **UAS flyability** to demonstrate our scenarios. The UAS platforms were not consistently reliable when attempting to fly them directly out of the box, which is likely how a public safety or commercial operator would implement them. Prior to implementing our scripts on the UAS platforms, we performed initial test flights and encountered issues with the connection between the GCS and UAS. We also found that calibration and tuning was needed for the platforms to allow better control and responsiveness of the UAS during flight.

This project marked our first attempt at demonstrating the BFDI-AP system capabilities on **commercial-off-the-shelf (COTS) UAS platforms**, including vendor-built software and hardware configurations with varying degrees of flexibility. Our original prototype was configured and demonstrated using a custom-built UAS platform that provided flexibility in the system configuration. To account for the additional complexity of adapting the BFDI-AP system to work with COTS platforms, we dedicated extra time in the earlier research phase to inspect the platforms and become more familiar with the configurations, especially those necessary for system operation. Following our BFDI-AP system updates, we dedicated extra time in the project schedule for multiple rounds of testing to allow for iterative improvements to the BFDI-AP system.

Our BFDI-AP system is designed to protect UAS platforms from compromise by bad actors who may seek to disrupt UAS operations by public safety personnel, commercial operators, and other users. To demonstrate the value and effect of our solution, our original demonstration plan called for the unsecured UAS platform to be compromised during flight. However, this approach presents numerous **safety, security, and policy concerns**, including the potential for bystanders to be injured by loss of control of the UAS and the similarity of this testing to be construed as UAS mitigation, which is solely under the jurisdiction of the US Department of Homeland Security. In light of this challenge, we adapted our demonstration plan to focus instead on explaining (rather than conducting) the potential cybersecurity compromise and then demonstrating that the operation and capabilities of each of the UAS platforms was not affected by the application of the countermeasures from the BFDI-AP system.

We also faced **supply chain delays** for several components of our project. The UAS platforms we planned to acquire and several hardware components for our BFDI-AP system were on backorder because of supply chain delays caused by various events (e.g., the Russia-Ukraine war). To mitigate this challenge, our team reevaluated our project schedule, identified key activities dependent on these items, and adjusted our timelines to account for the delays. We also moved other project activities earlier in the schedule to remain productive while waiting for our items to arrive.

For any live outdoor demonstration, the **weather** will always be a potential challenge. In the case of this project, our demonstration focused on conducting multiple UAS flights, and each of the UAS platforms has different tolerances for the level of wind, rain, and other weather conditions that can be overcome to produce a safe flight. As an initial mitigation, we scheduled a full week at the New York UAS Test Site to allow for rescheduling if adverse weather was expected during our planned event days. This proved valuable because scattered thunderstorms were forecast throughout the week of our demonstration. Working with the test site, we reviewed the forecast for each day and planned our events accordingly. Even with this mitigation, our team had to end some of our testing early because of weather conditions including a severe thunderstorm and a tornado.

Another challenge our project team encountered was known from the start—that we were a **distributed project team** that would need to have in place processes to complete our project objectives effectively. Our project team members were located in four states geographically dispersed across the US (Virginia, Florida, Michigan, and New York). To mitigate the potential effects of this dispersion, we established collaboration tools for asynchronous project tasking, held regular team meetings using virtual meeting platforms, and coordinated travel among the team to meet in person for key project milestones.

LESSONS LEARNED

Our experience on this project to advance the maturity of our BFDI-AP system for UAS cybersecurity resulted in several lessons learned that can be applied to improve outcomes in future projects. In some cases, these lessons learned served more as reinforcement of project planning best practices than revelations or discoveries, but nonetheless, they proved essential to the success of the project.

One lesson learned was that more work is needed to improve the usability and scalability of the BFDI-AP system for use by public safety and commercial operators. The user interface for the BFDI-AP was improved over the course of the project, but further improvements can be made based on our experience with the COTS products. For example, one of our countermeasure scripts requires the operator to manually update the new encryption settings in the GCS to match those applied to the UAS. For usability among operators and scalability to larger UAS fleets, this type of process must be automated so the operator can ensure that use of the system will secure the full fleet without relying on additional manual processes.

Through the course of this project, we also learned the value of testing on COTS products to advance the technology readiness level of system or capability prototypes. Our initial development work on our BFDI-AP system before this project focused on demonstrating the system's capabilities using a custom-built UAS platform, which allowed our team control and flexibility in the system configuration. When looking to advance and mature the prototype for real-world operations, it is imperative that the system can work with COTS products that would be used in these operations and still maintain ease of use for the operator. For example, we found that developing our updated cybersecurity scripts for COTS UAS platforms required additional settings to account for commercial radio configurations and additional steps to ensure that our solution still provided the intended cybersecurity protections.

We learned the value of UAS test flights to validate the nondestructive nature of cybersecurity solutions such as the BFDI-AP system. The BFDI-AP system is intended for use as a preventive measure to secure a UAS platform through configuration updates. As such, the countermeasures are applied to the UAS platform on the ground before flight operations, and the operations of the BFDI-AP system itself can be fully demonstrated without flying the UAS platform. However, by flying the UAS after applying these measures to the platform, we were able to demonstrate effectively that our cybersecurity scripts did not alter or degrade the capabilities of the UAS platform.

Finally, we learned the value of advanced planning and logistics for a demonstration project among a geographically distributed team. Although recent technological advancements have vastly improved the capabilities for project teams to collaborate remotely (especially in the last few years as a result of the COVID-19 pandemic), there were additional factors to consider for this project. For example, this project required our UAS platforms to be available at multiple locations to facilitate the required hands-on development and testing tasks. This included shipping the platforms to the RIIS facility in Michigan for vulnerability assessment and flight testing, another RIIS facility in Florida for hardware and troubleshooting tasks, the NUAIR facility in New York for final flight testing and inspection, and then finally to the New York UAS Test Site (in a different city in New York) for final demonstration. These shipping tasks must be accounted for in the project schedule.

A related lesson learned was the value of in-person meetings for distributed teams to meet key project milestones or significant activities. Again, technological advancements have created an environment where most project activities can be conducted seamlessly through virtual platforms. However, we found that several strategic trips to assemble the project team in person were instrumental in keeping the project on track. This was exemplified by our team trip to the RIIS facility in Michigan for final system testing and flight testing. We encountered a few final issues with our cybersecurity scripts that required troubleshooting, and the ability of the team to be co-located increased the efficiency and effectiveness of these sessions.

RECOMMENDATIONS AND NEXT STEPS

Following the various phases and completion of the final demonstration, the CNA team has developed recommendations for how the project's research can be used to advance UAS cybersecurity. They include the following:

- Increase awareness of common security misconfigurations that could be present and exploited in the UAS community. As detailed in this report, default settings are one of the easiest and most common ways for malicious actors to gain access to a platform or system. Default configurations should always be changed on the UAS prior to operations.
- Recommend to UAS manufacturers that they include instructions for updating default configurations and credentials in the user manuals. A good practice would be to provide brief, user-friendly instructions early in the "setting up your device" section that describe to the user both how and why to update the default settings. Emphasizing why security is important for the device may help incentivize the user to complete the process during the initial set up phase.
- Call attention to design considerations for UAS to account for strong security configurations. There may be times when increasing the security on a given platform either conflicts with or inhibits the system's full functionality. We observed this issue while testing the UAS: RFD900 drone. Changing the drone's radio network disabled the GPS module because of the design of the components.
- Present the findings in this report as well as from previous projects as validation of the BFDI-AP system's value for securing UAS. For smaller organizations within the public safety and commercial sectors, the BFDI-AP offers a streamlined, user-friendly approach to securing sUAS that requires very little technical knowledge. For organizations that need to get their drones operational quickly after receiving them, the BFDI-AP offers a fast method for increasing the security of a small sUAS fleet.
- Bring awareness to security issues that may exist within sUAS that have been accepted on the DIU's Blue UAS List as well as AUVSI's Green List. Although these systems have been vetted and are deemed compliant with section 848 of the FY 2020 NDAA, Section 817 of the FY 2023 NDAA, and the American Security Drone Act, they still may have poor default security settings that require additional user reconfigurations to secure the device properly.

In addition to these recommendations for UAS cybersecurity, we have looked into the next steps to continue to advance our BFDI-AP system. Based on the challenges and lessons learned from this project, we would prioritize usability and scalability updates that would allow the application of this system to large UAS fleets for public safety and commercial operators. We will perform more research on the signal interference issue that we experienced in our test lab since the intended use of the BFDI-AP system would likely be in an indoor setting that could include similar interfering signals. Finally, our research focused on

COTS platforms that are DIU Blue List or AUVSI Green List compliant; however, based on the outcomes of future federal and state legislation regarding the use of certain foreign-made UAS, we would look to test additional UAS platforms that comprise a large portion of the current UAS market.

FIGURES

TABLES

ABBREVIATIONS

AUVSI	Association for Uncrewed Vehicle Systems International
BFDI	Brute Force Default Identification
BFDI-AP	Brute Force Default Identification-Automated Prevention
C2	command and control
CNA	CNA Corporation
CNA-RIIS team	CNA partnership with software company RIIS
COTS	commercial-off-the-shelf
DIU	Defense Innovation Unit
DOD	Department of Defense
FAA	Federal Aviation Administration
GCS	ground control station
NDAA	National Defense Authorization Act
UAS	uncrewed aircraft system
sUAS	small uncrewed aircraft system

REFERENCES

[1] “Blue UAS.” n.d. DOD Innovation Unit. https://www.diu.mil/blue-uas.

[2] “First Responder UAS Triple Challenge—Shields Up! Securing UAS Navigation & Control (UAS 3.3).” NIST. Aug. 11, 2022; updated Sept. 28, 2022. https://www.nist.gov/ctl/pscr/open-innovation-prize-challenges/past-prize-challenges/2021-first-responder-uas-triple-1.

[3] Houssam Abbas et al. “UAS Cyber Security and Safety Literature Review.” ASSURE. Nov. 23, 2021. https://assureuas.org/wp-content/uploads/2021/06/A38_Literature-Review_FINAL.pdf.

[4] “Green UAS.” n.d. Association for Uncrewed Vehicle Systems International. https://www.auvsi.org/green-uas.

[5] National Defense Authorization Act for Fiscal Year 2024. 118th Congress. S.2226. July 27, 2023. https://www.congress.gov/bill/118th-congress/senate-bill/2226.

[6] “Cyber Kill Chain.” Lockheed Martin. 2023. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

This report was written by CNA's Enterprise Systems and Data Analysis Division (ESDA).

CNA's Enterprise Systems and Data Analysis division (ESDA) creates advanced, integrated enterprise systems and data management solutions that empower clients to make decisions at pace with the speed and scale of their mission. ESDA analyzes the entirety of systems—the people, the process, the data, and the technology—to improve the efficacy of operations through optimized data-driven environments.

This report may contain hyperlinks to websites and servers maintained by third parties. CNA does not control, evaluate, endorse, or guarantee content found in those sites. We do not assume any responsibility or liability for the actions, products, services, and content of those sites or the parties that operate them.

ABOUT CNA

CNA is a nonprofit research and analysis organization dedicated to the safety and security of the nation. It operates the Center for Naval Analyses—the federally funded research and development center (FFRDC) of the Department of the Navy—as well as the Institute for Public Research. CNA develops actionable solutions to complex problems of national importance. With nearly 700 scientists, analysts, and professional staff, CNA takes a real-world approach to gathering data. Its unique Field Program places analysts on aircraft carriers and military bases, in squad rooms and crisis centers, working side by side with operators and decision-makers around the world. CNA supports naval operations, fleet readiness, and strategic competition. Its non-defense research portfolio includes criminal justice, homeland security, and data management.

CNA

Dedicated to the Safety and Security of the Nation

www.cna.org